Consolidated Records Management System

a joint effort between the Tennessee Bureau of Investigation and the Tennessee Office of Homeland Security

CRMS Audit Feature Introduction

Scheduled for implementation on June 1, 2011

CRMS Audit Feature Purpose

CRMS access and use of the system is restricted to law enforcement officials or those persons supporting law enforcement.

CJIS Audit requirements include the collection of information relative to the use of Criminal Activity systems and information.

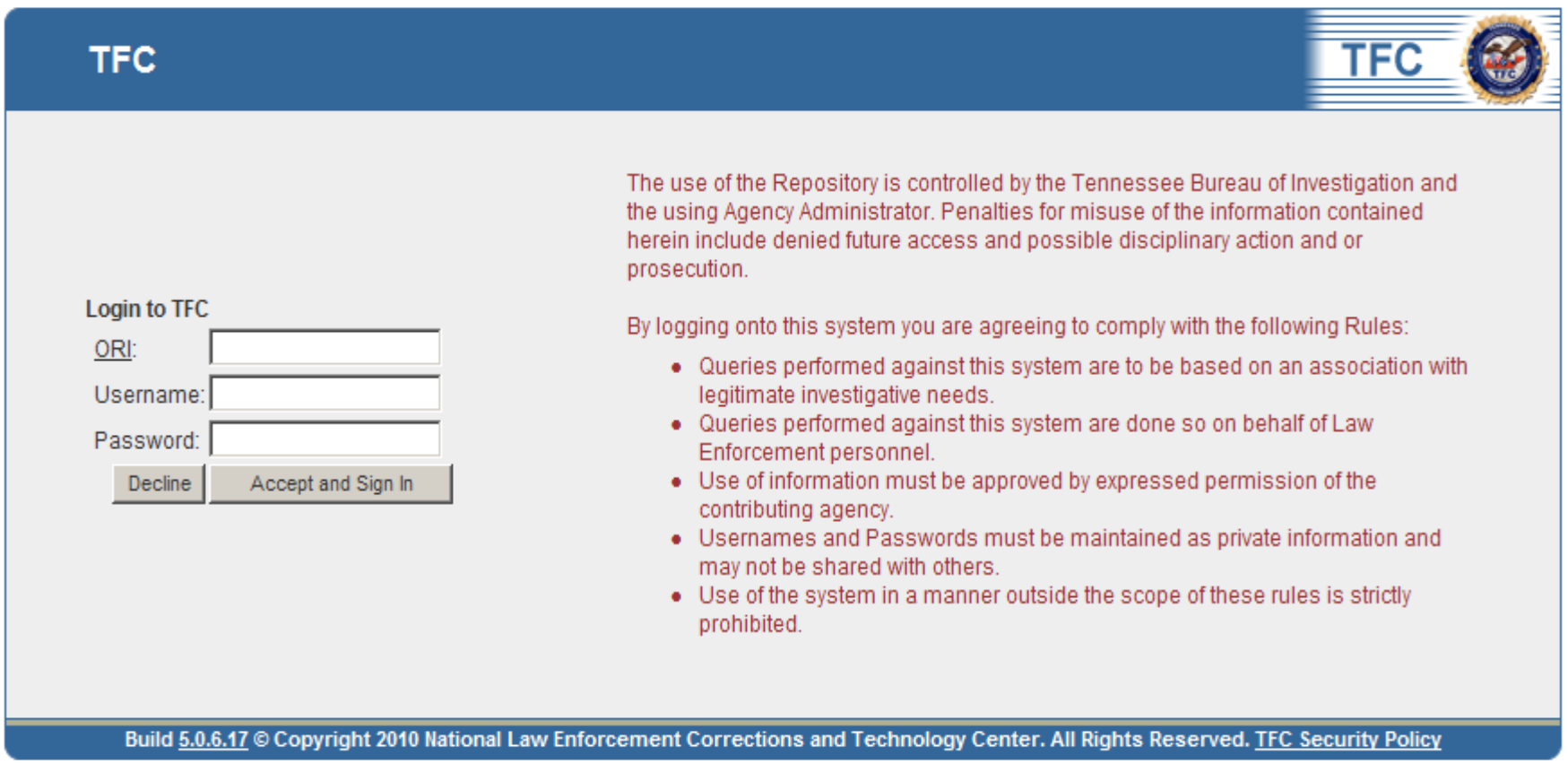
Criminal Activity systems must collect four items of information for searches done within the system:

1. The name or badge number of the officer requesting the information.
2. Distribution of the information or who gets the information.
3. The reason the search is performed, perhaps a case number or traffic stop.
4. The User ID of the person performing the search (the user that is logged on the system).

The system now has 3 new fields on the search panels to meet the CJIS requirement. These free-form text fields collect 1) Query for Agent, 2) Dissemination to, and 3) Query Reason. The user id (4) is automatically collected as the user logs into the system.

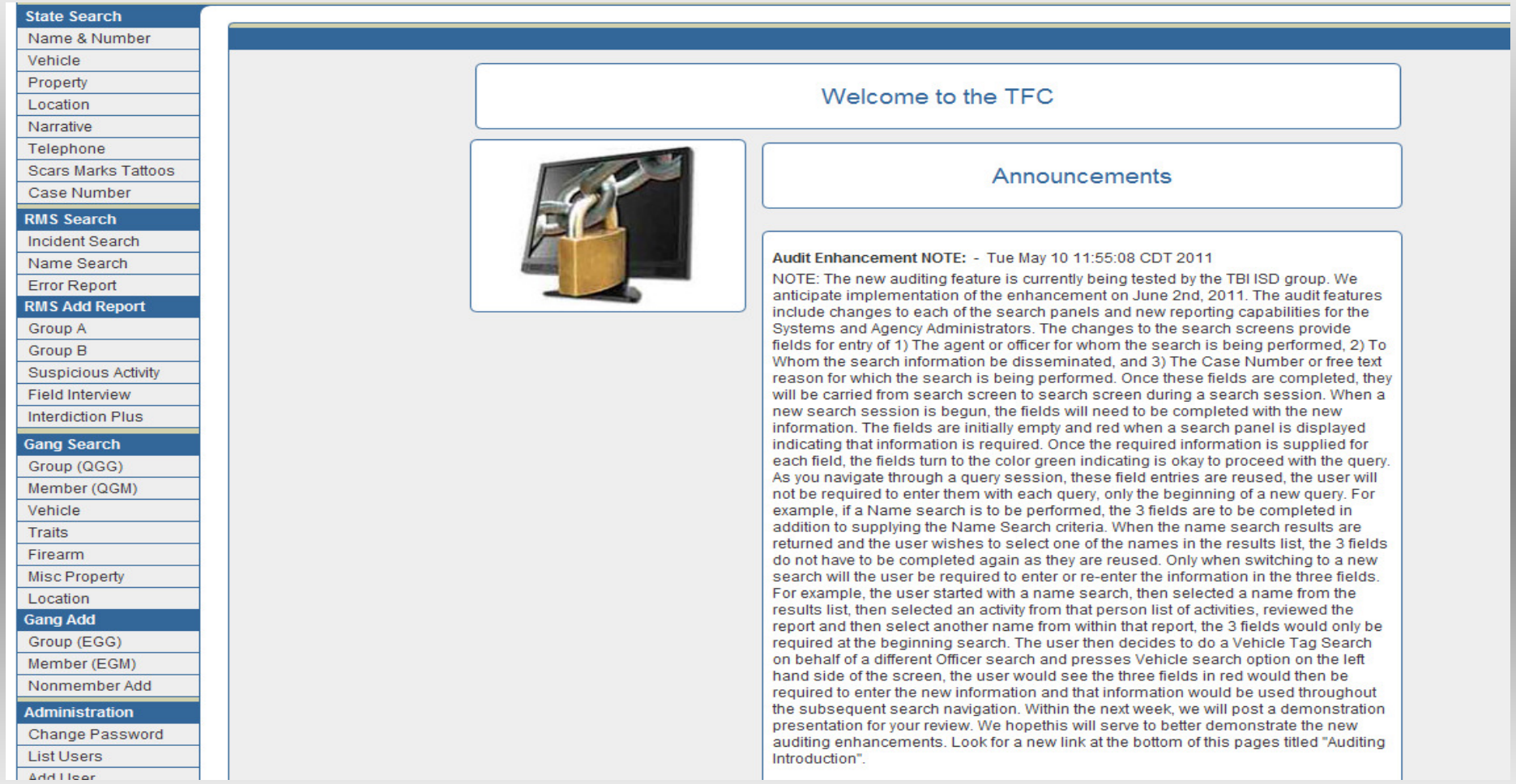
Each agency can establish a standard for field content if they wish, i.e. always use badge number, etc.

CRMS Use Disclaimer



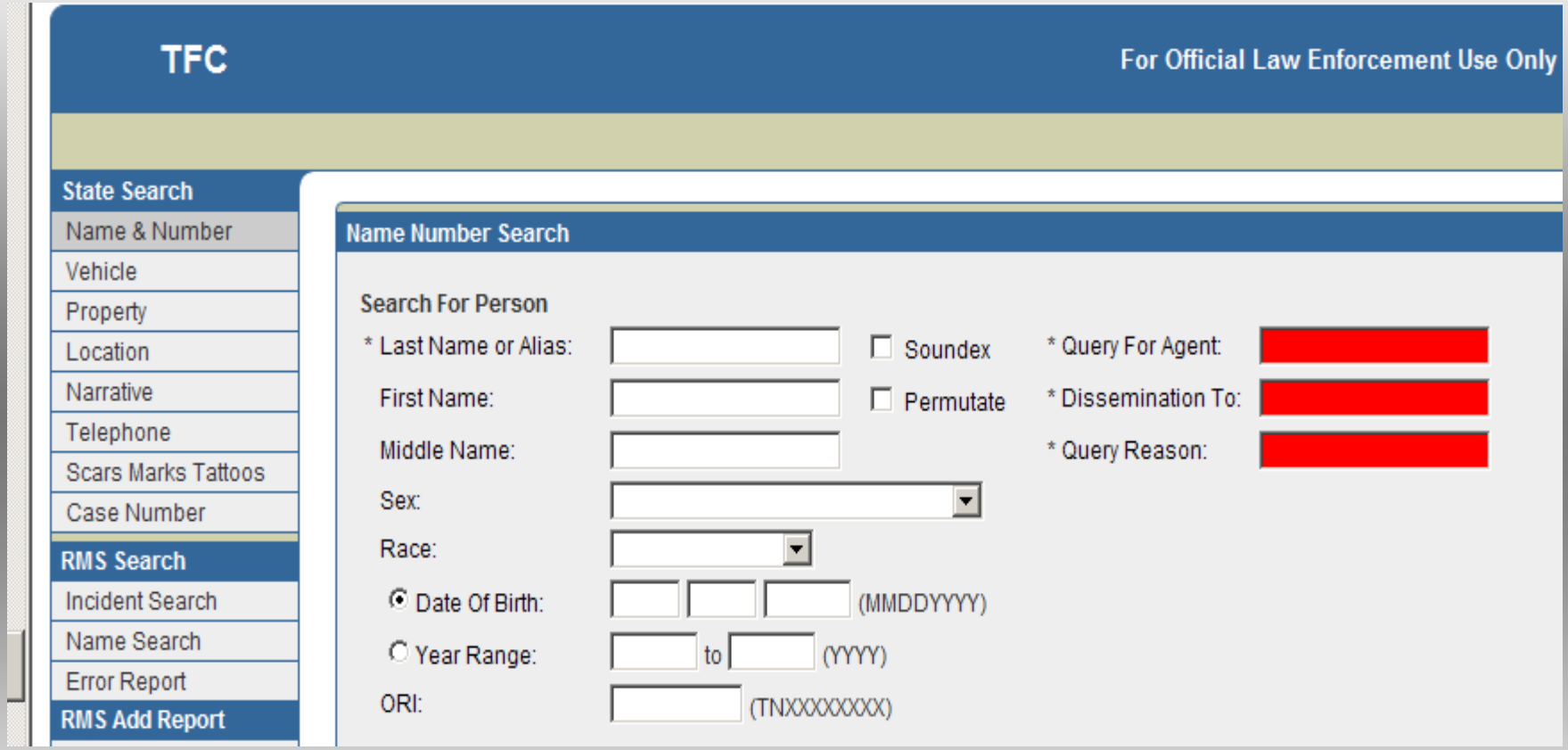
Rules of Use are displayed on the Home Page of the system and logging into to the system constitutes agreement with those rules.

CRMS Announcement Page

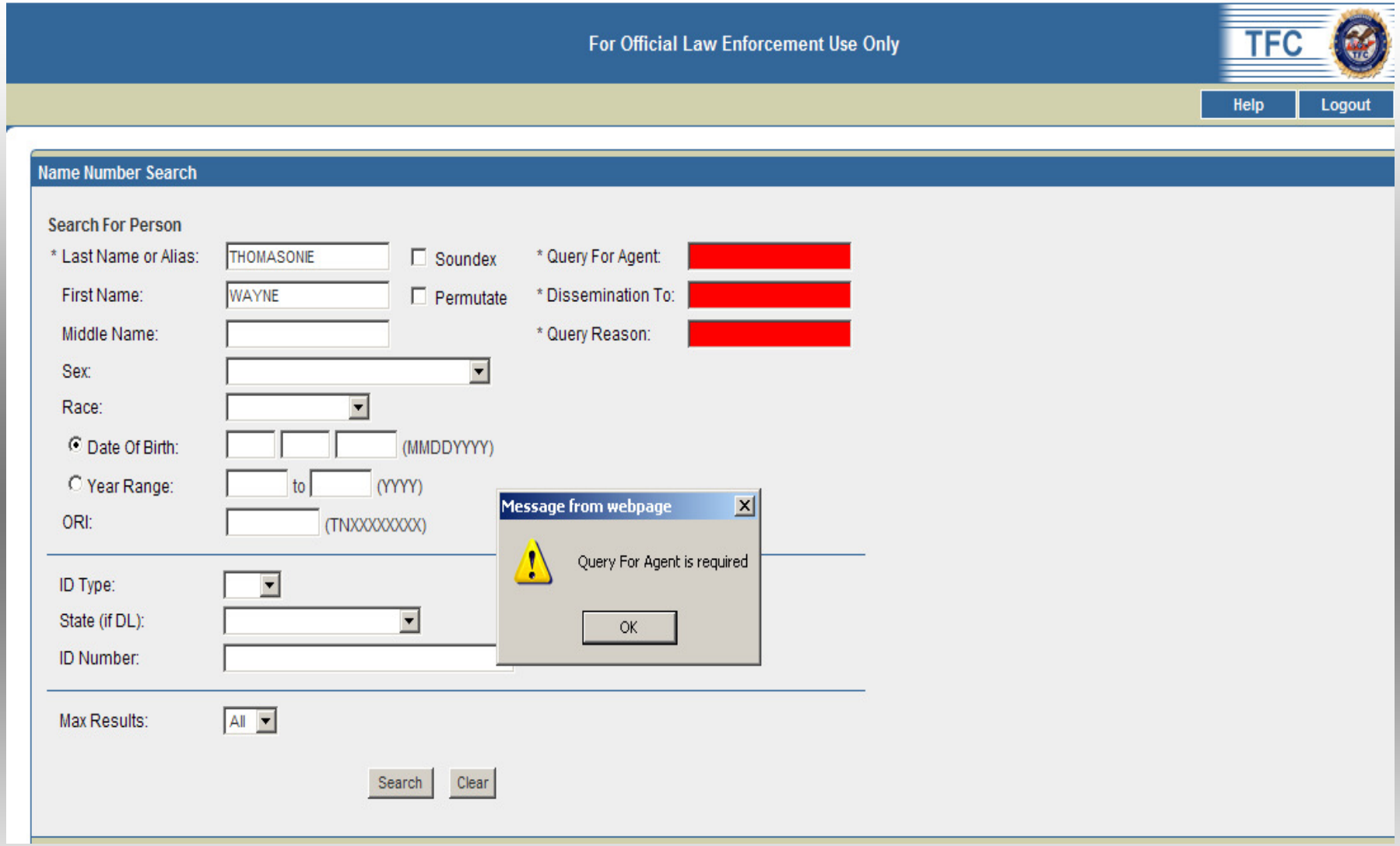


Once logged onto the system, the announcement page is shown to notify users of any changes to the system. This announcement highlights the Audit Enhancement.

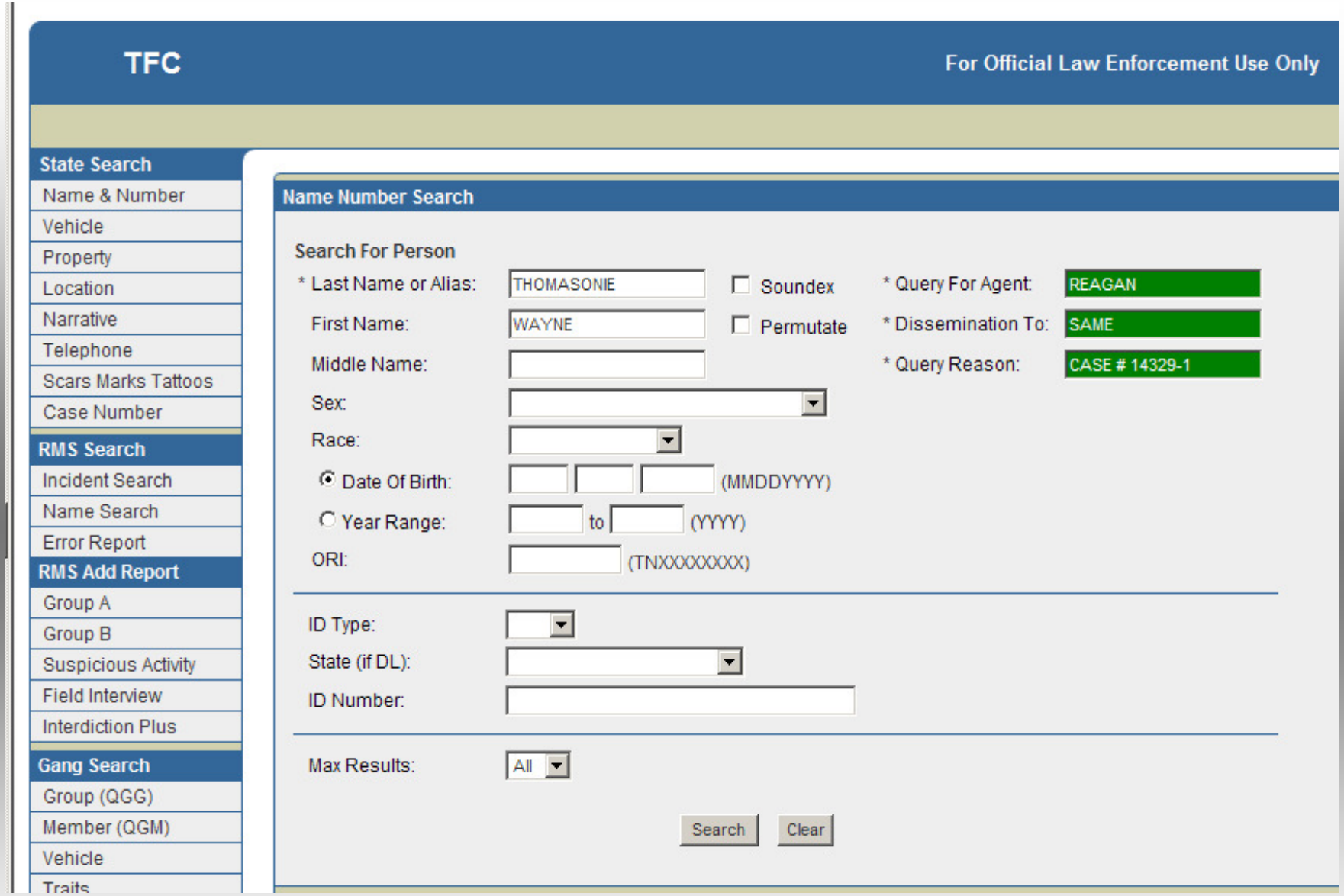
New Audit information collection fields



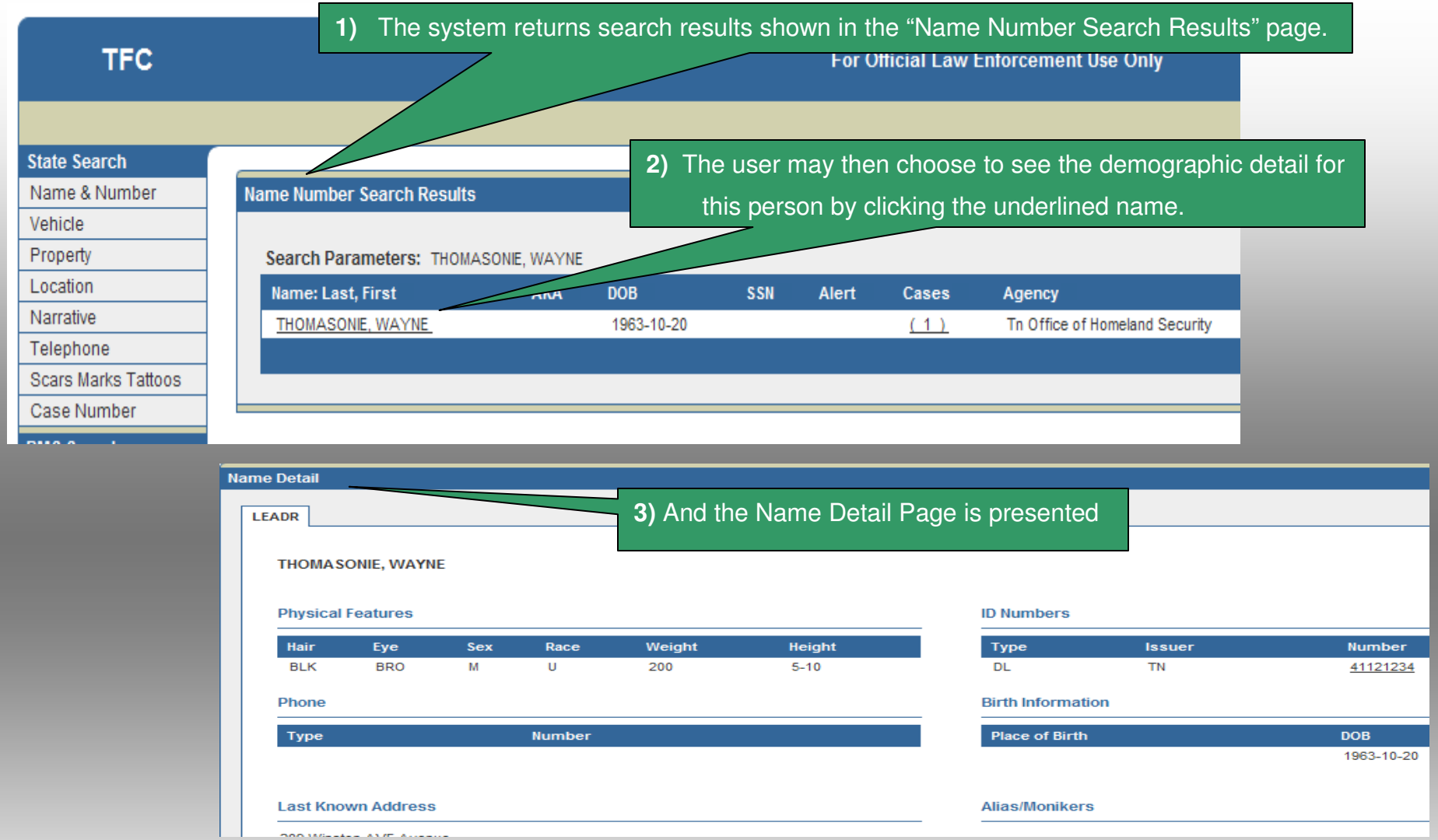
- The new audit information collection fields are shown on each of the State Search Panels. The audit information is not required for RMS Searches or RMS Add Report functions as these are functions specific to an individual agency's use of its own information.
- This illustration shows the fields highlighted in red indicating information is required before the search can be performed.



- The audit information fields are mandatory and must be supplied before a search can be performed.
- If a search is attempted without the required information in the audit fields, the system produces an error message indicating the field to be supplied by the user.

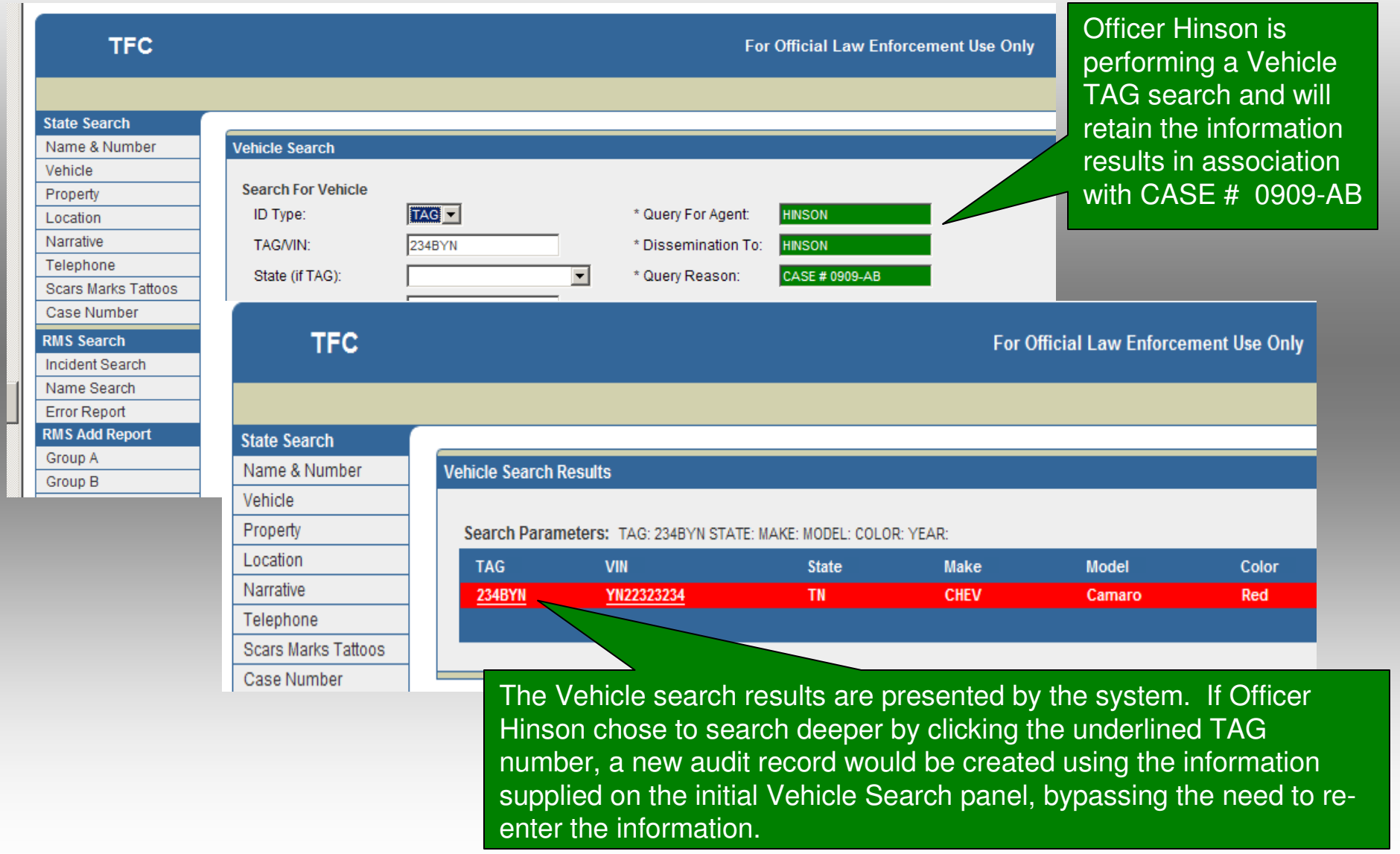


- This illustration shows the fields highlighted in green indicating the required information has been supplied and the user may proceed with the search.
- In this case, Officer Reagan has requested a search be performed and the results will be used by himself in association with case # 14329-1.



- The three audit fields follow the search chain. The contents of the audit fields apply to all actions performed after the initial search request.
- For instance, an audit record was written for the initial "Name and Number" search and another audit record is written for the "Name Detail" search. Each audit record uses the information supplied on the initial "Name & Number" search panel, bypassing the need to re-enter the information.

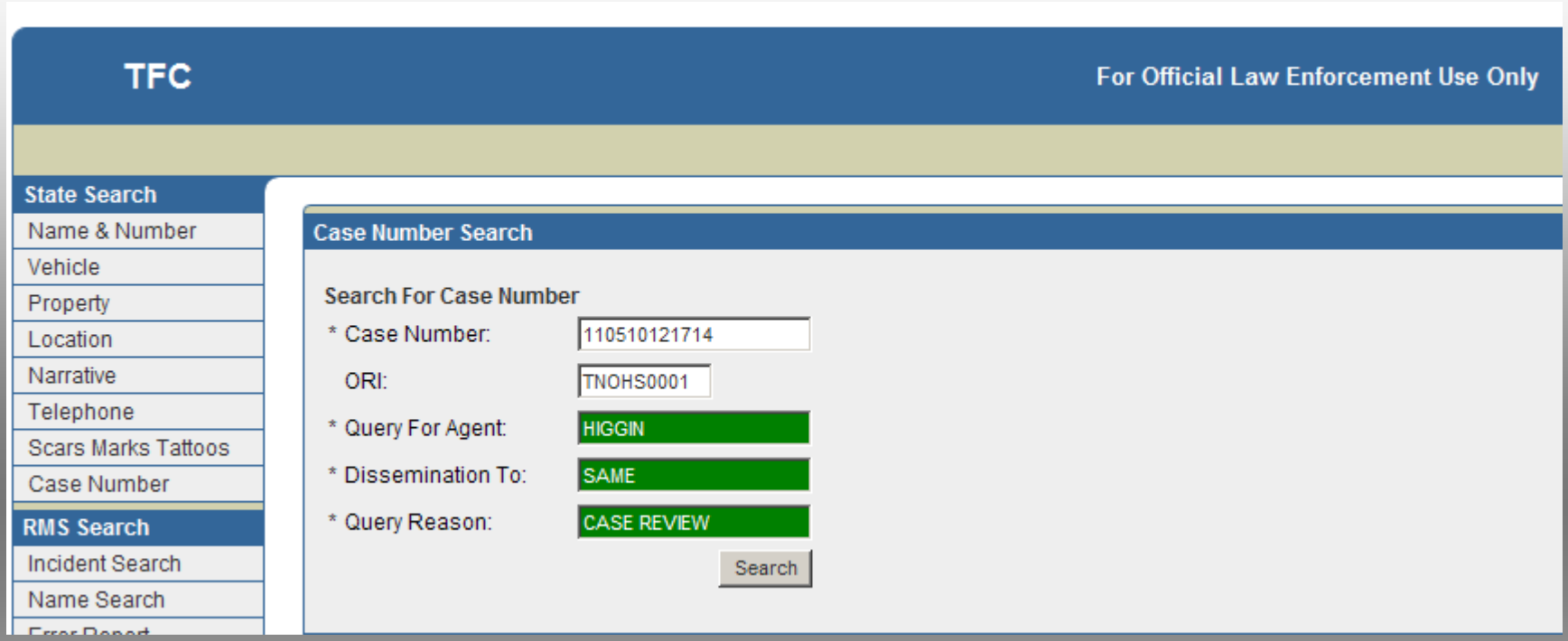
Vehicle Search



Officer Hinson is performing a Vehicle TAG search and will retain the information results in association with CASE # 0909-AB

The Vehicle search results are presented by the system. If Officer Hinson chose to search deeper by clicking the underlined TAG number, a new audit record would be created using the information supplied on the initial Vehicle Search panel, bypassing the need to re-enter the information.

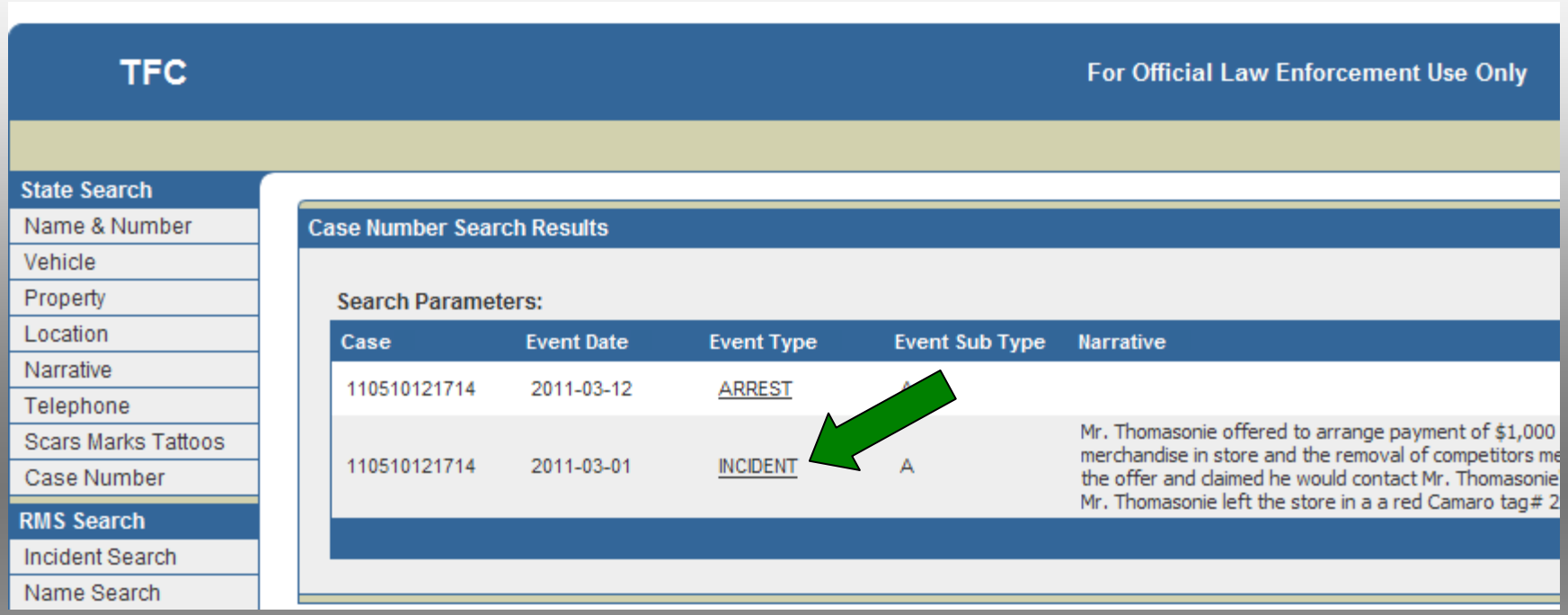
Case Number Search Scenario



- The user is performing a search for a specific case number to identify information associated with the case on behalf of Investigator Higgin. Higgin will retain the information for the case review.

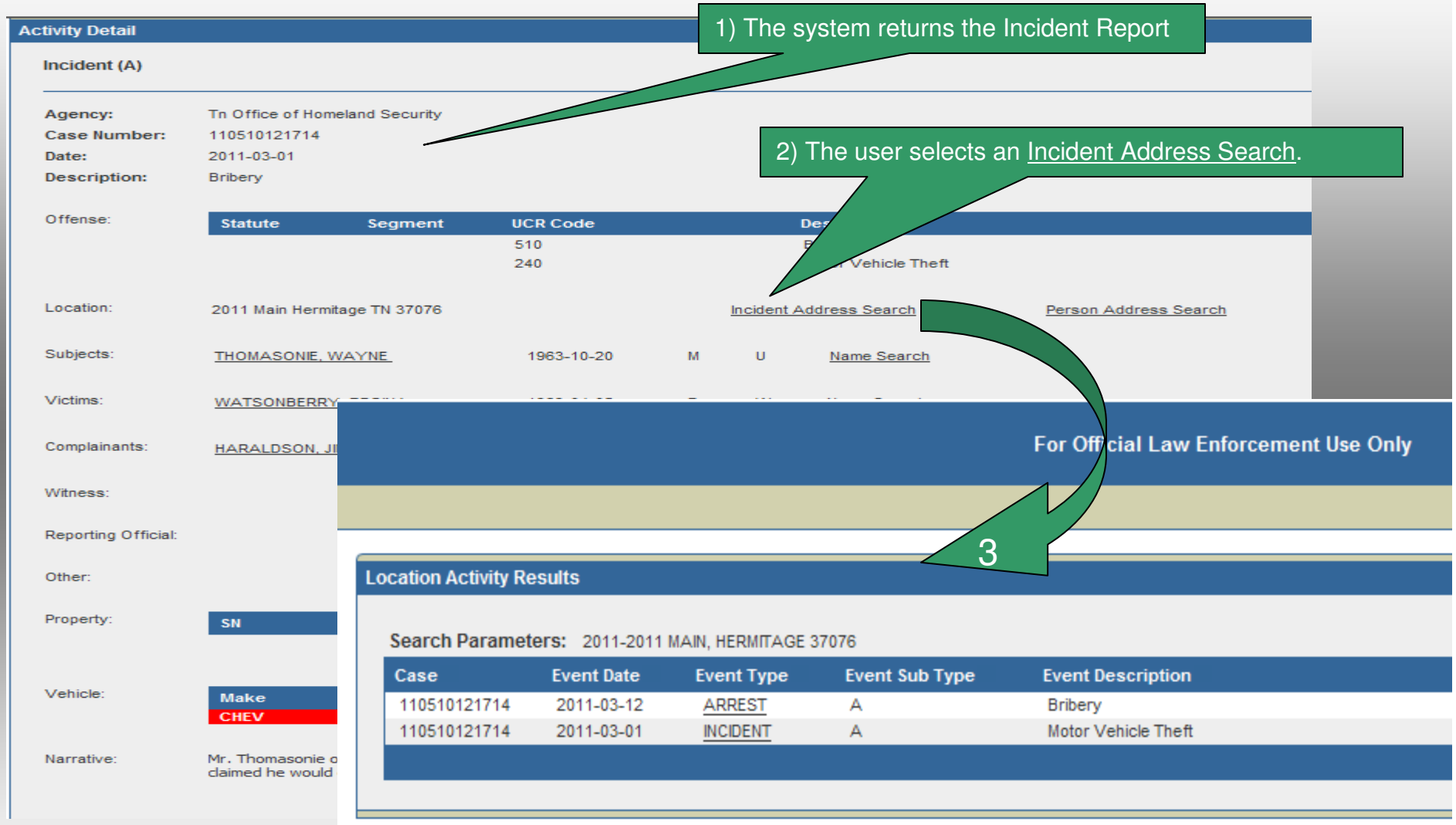
- Investigator Higgin wants to know:
  - about activities connected to the case, (Case Number Search)
  - where the incident took place, (Incident Report Search)
  - any other activities that have taken place at that location, (Location Search)
  - any other activity associated with the subject in the case. (Name Search)

Case Number Scenario



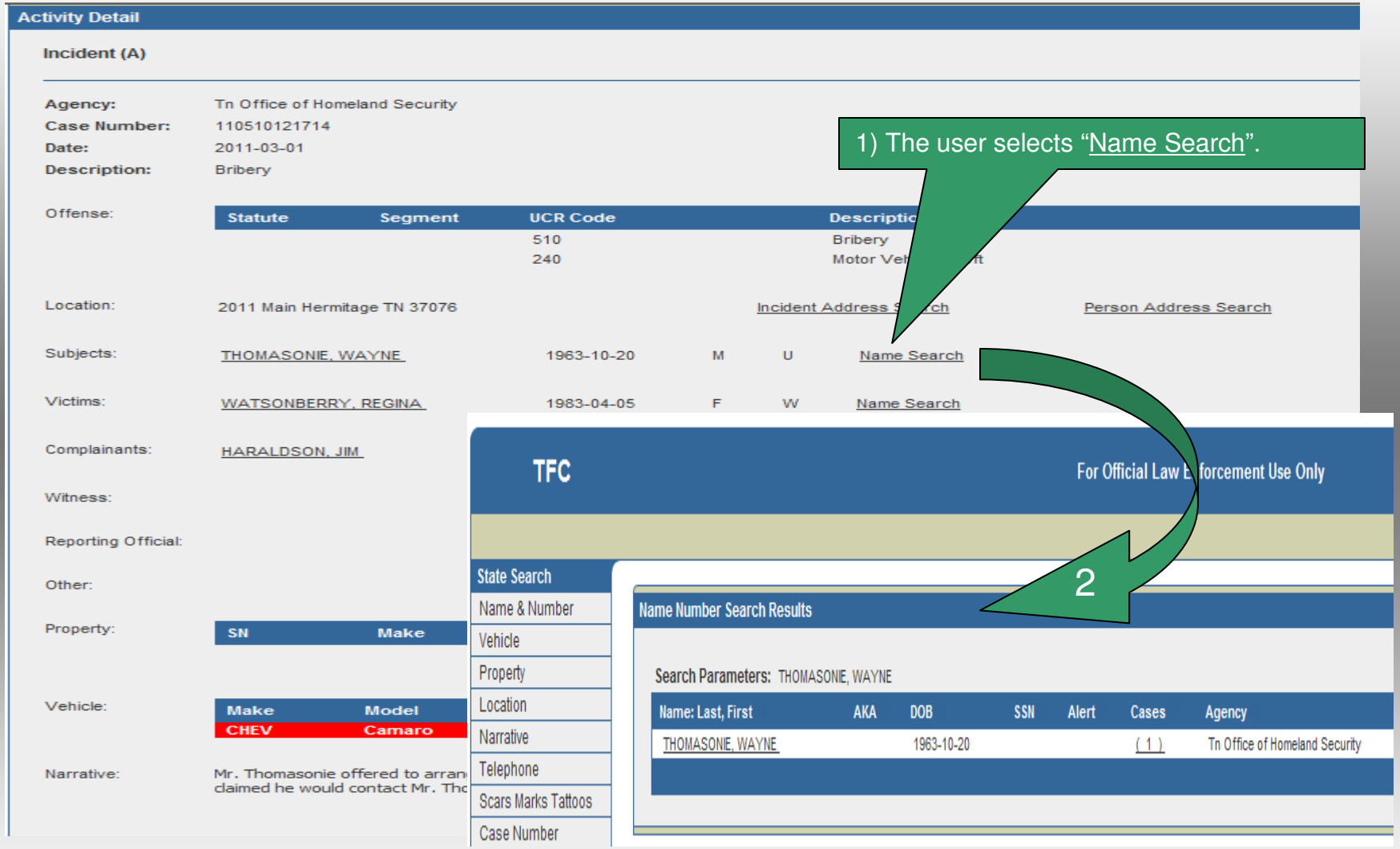
- The system returns two activity records associated with case number 110510121714, an Incident Report and an Arrest report.
- To view the Activity details associated with the case, the user selects the underlined Incident Activity. Re-entering the audit information is not required.

Case Number Scenario



- 1) Next, the user wants to know if other activities have taken place at this location, so the user clicks the underlined "Incident Address Search". The initial audit information will be re-used as this search is still part of the initial search request.
- 2) The system provides a list of activities that are associated with the selected address.

Case Number Scenario



- 1) Next, the user wants to know if other activities are associated with the Subject and clicks the appropriate underlined "Name Search". The initial audit information will be re-used as this is still part of the initial case number search request.
- 2) In this instance, only one case is associated with the subject.

- In the Case Number search scenario, the Audit information fields were supplied at the initial point of the search chain, Case Number Search and then reused for each additional search or information request performed by the user:

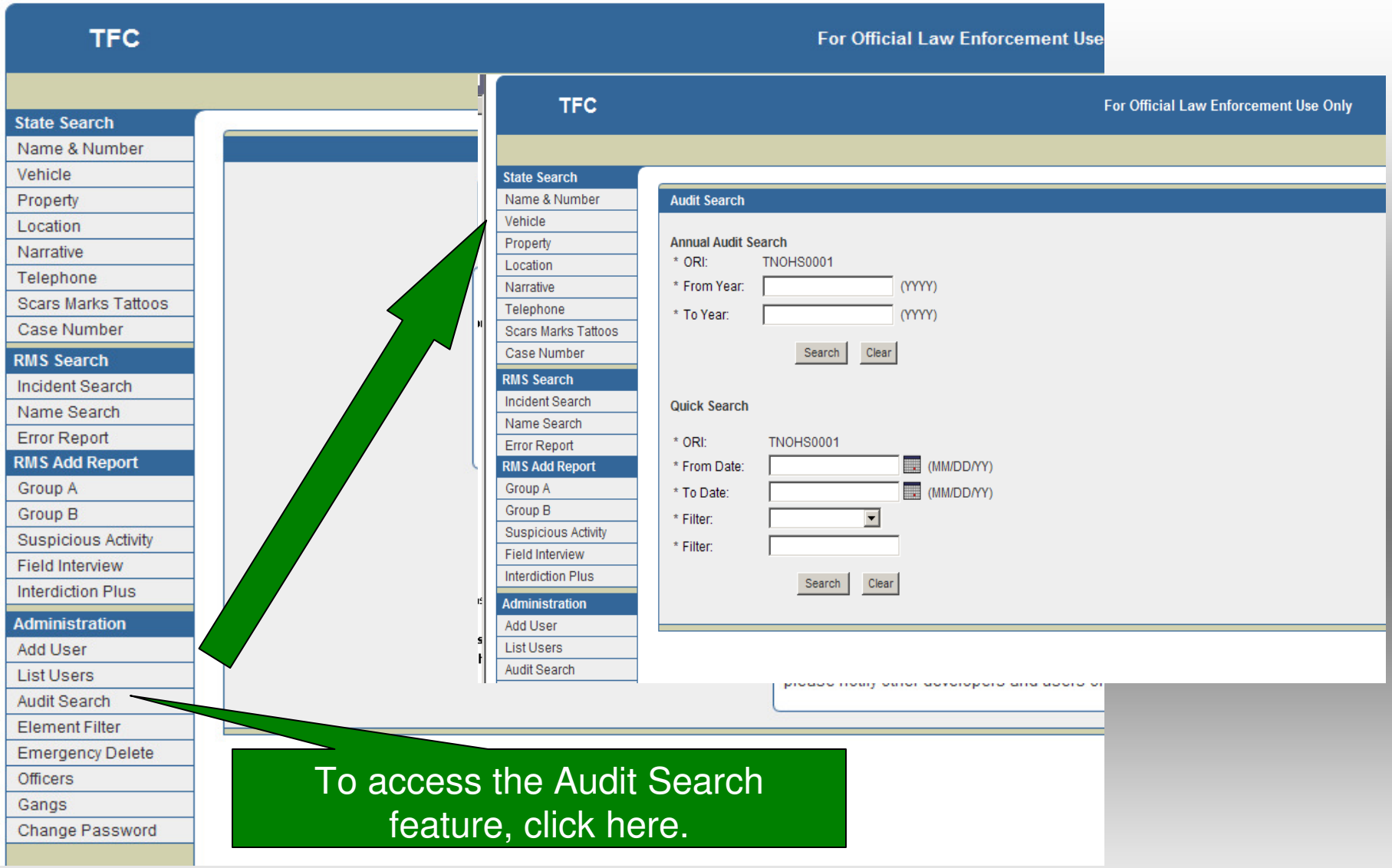
1. Initial Case Number Search (Supplied Audit Information)
2. Incident Detail Search (Information Re-Used)
3. Incident Address Search (Information Re-Used)
4. Incident Subject Name Search (Information Re-Used)

- An audit record was written for each search performed.

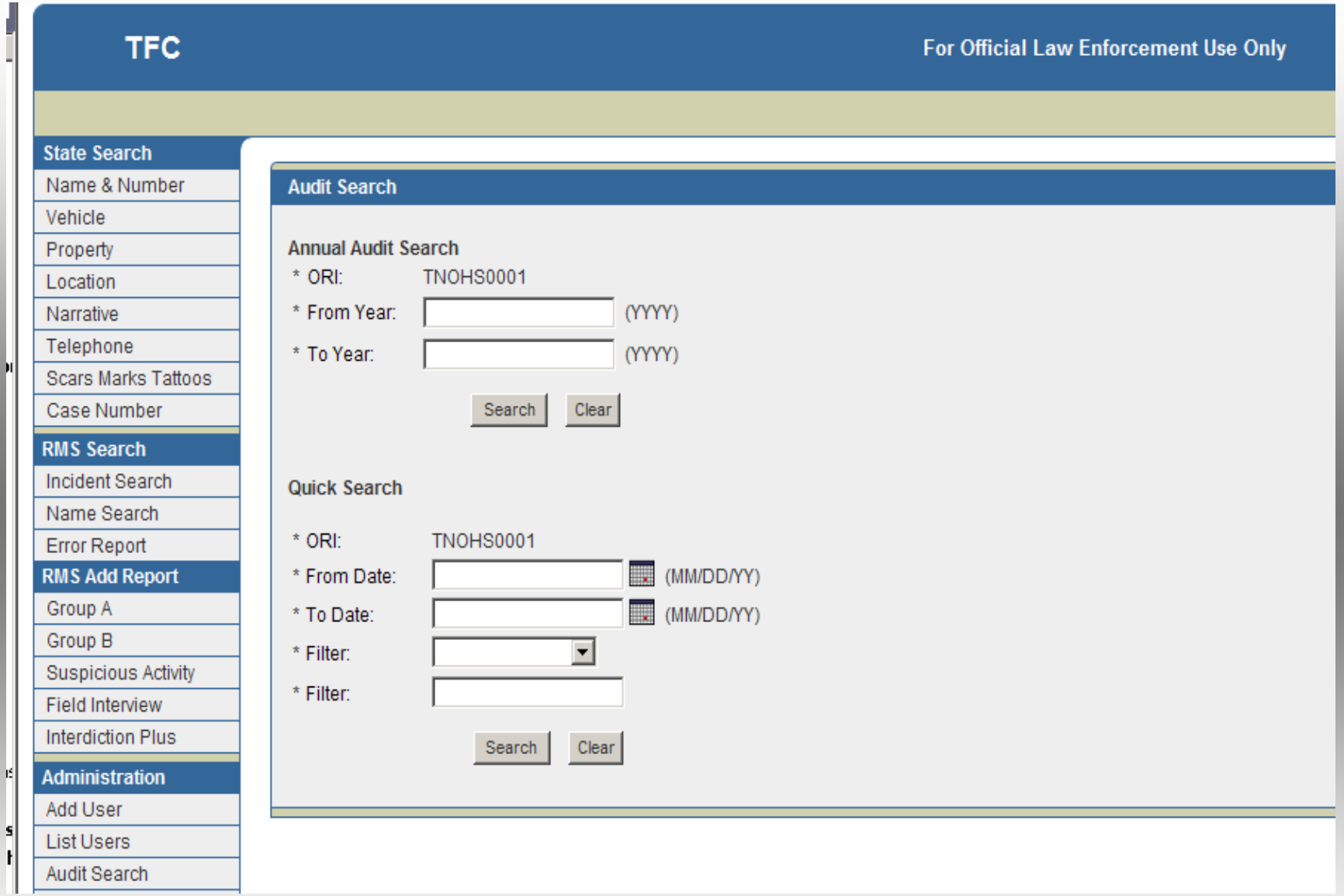
Reviewing Audit Reports

- Agency Administrators as well as the System Administrator have access to the Audit Data Search function.

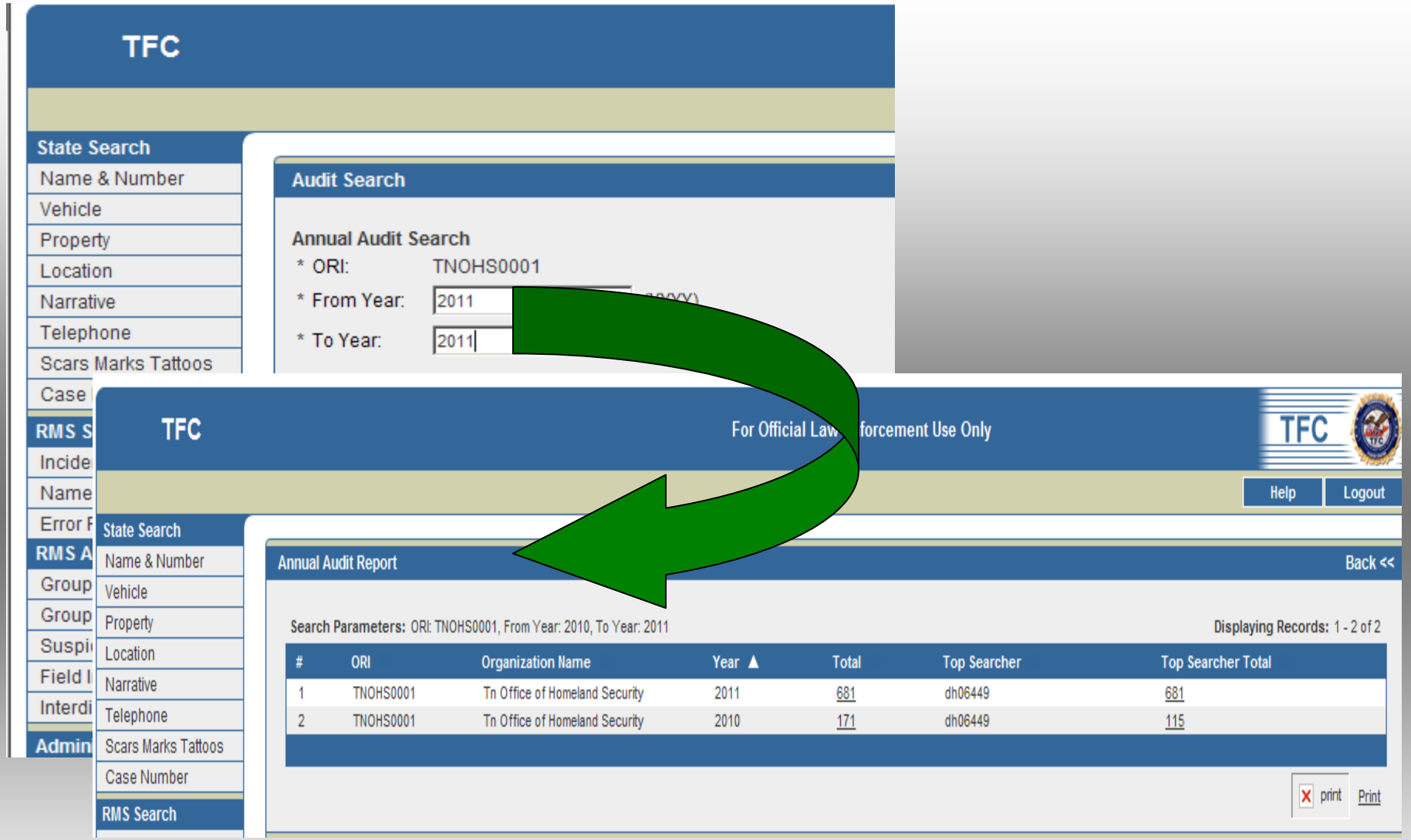
- The Audit Search function provides:
  - Annual Review of all audit data performed by all users within the agency.
  - Audit data for specific search activity, such as who searched for a specific tag number or who searched for a specific person name.
  - All searches performed by a specific user.



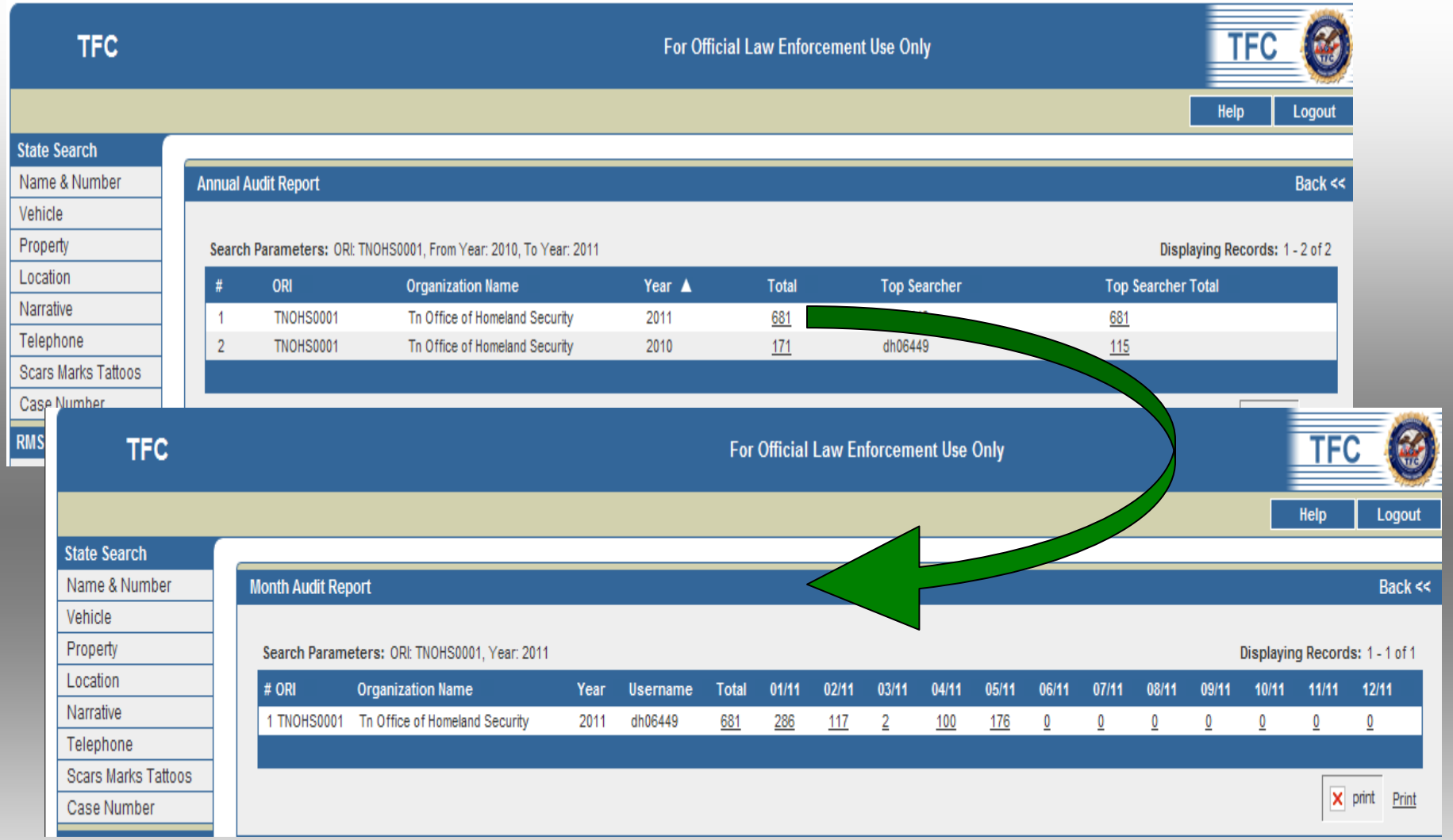
- Accessing the Audit Review feature from the Administration section.
- Only Agency Administrators has access to this feature.



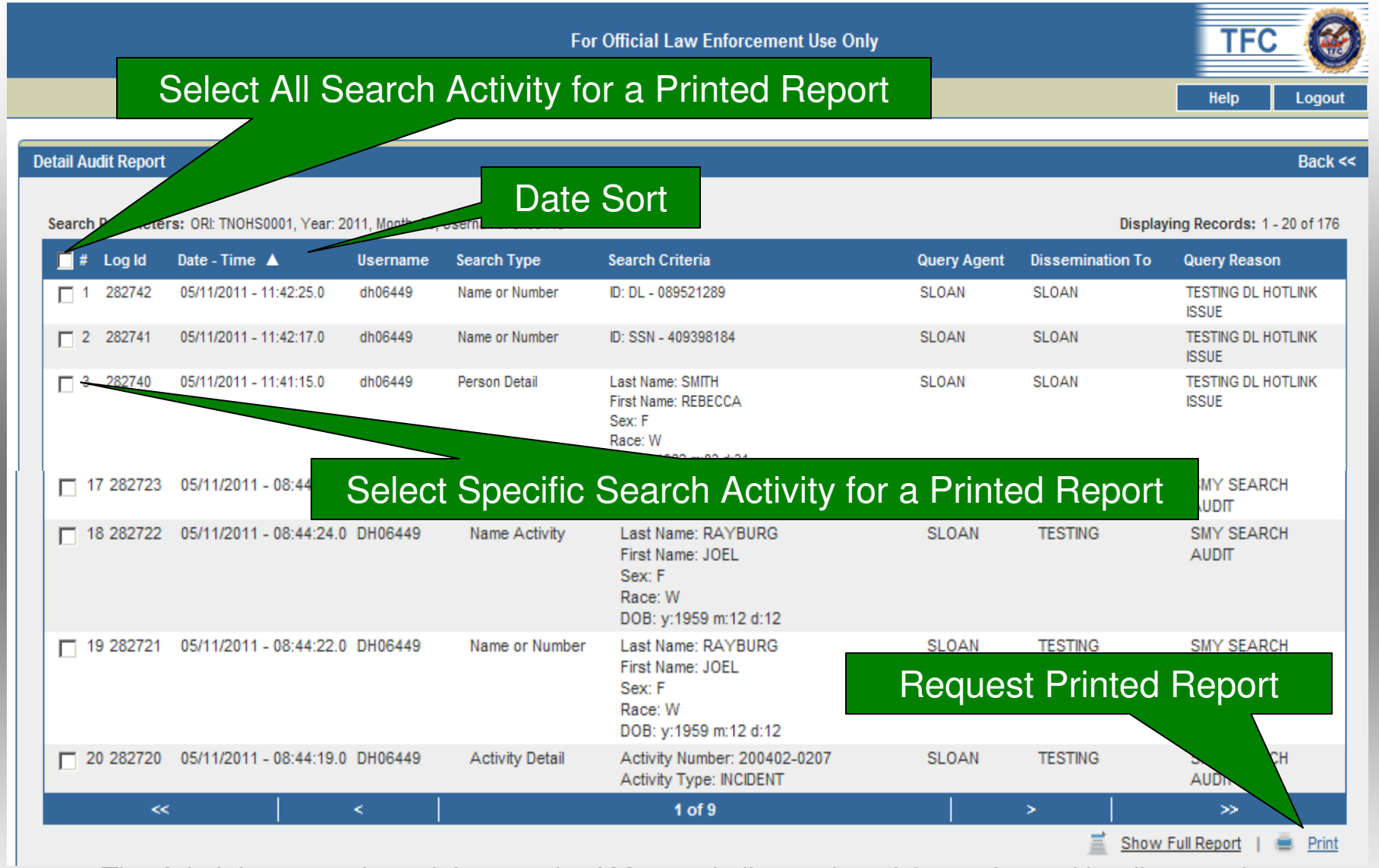
- The Audit Search panel offers two search options:
  - Annual Audit Search allows the administrator to view a spreadsheet of monthly use by all users within the agency.
  - Quick Search allows the Administrator to search audit records for activity against a specific tag, name searches or all searches performed by a specific user.



- The Administrator for ORI TNOHS0001 wishes to see all activity for all users within that agency for the years 2010 and 2011 and the system provides the annual report.
- The report shows dh06449 as the user with the highest number of searches, with 171 search activities in 2010 and 681 search activities in 2011..
- From this report, the Administrator can request a summary for a user by clicking on the underlined activity total.



- The Administrator requested a review of monthly activity for user id dh06449 and the system gives a report showing the count of search activities by month for the selected year.
- The Administrator can now look at the detail activity searches performed by user dh06449 by selecting the count for a given month.



- The Administrator selected the month of May and all search activity performed by dh06449 is illustrated.
- The Administrator can sort the list by date.
- The Administrator can also create a printed report showing all or specific searches.

Questions?

Please email questions or comments concerning this feature enhancement to:

TnCop.HelpDesk@tn.gov

When sending the email, please include the word “AUDIT” in the subject line of the email. Your email will be answered within 48 hours.